ДЕРЖАВНИЙ ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
“УЖГОРОДСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ”
ІНЖЕНЕРНО-ТЕХНІЧНИЙ ФАКУЛЬТЕТ
КАФЕДРА КОМП’ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

ЗАТВЕРДЖУЮ
Декан інженерно-технічного факультету
_____ доц. Йолана ГОЛИК
“__” _____ 2025 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ЗАХИСТ ІНФОРМАЦІЇ В КОМП’ЮТЕРНИХ СИСТЕМАХ

Рівень вищої освіти – перший (бакалаврський)
Галузь знань – 12 – інформаційні технології
Спеціальність – 123 – Комп’ютерна інженерія
Освітня програма – Комп’ютерні системи та мережі
Статус дисципліни – обов’язкова
Мова навчання – українська

Ужгород 2025

Робоча програма навчальної дисципліни «Захист інформації в комп'ютерних системах» для здобувачів вищої освіти галузі знань 12 – «Інформаційні технології» спеціальності 123 – «Комп'ютерна інженерія» освітньої програми «Комп'ютерні системи та мережі» – 17с.

Розробники: Гапак О.М., доцент кафедри комп'ютерних систем та мереж, канд. пед. наук, доцент.

Робочу програму розглянуто та затверджено на засіданні кафедри комп'ютерних систем та мереж

протокол № 13 від «25» червня 2025 р.

Завідувач кафедри _____ доц. Петро ГОРВАТ
(підпис) (прізвище та ініціали)

Схвалено науково-методичною комісією інженерно-технічного факультету

протокол № 6 від «27» червня 2025 р.

Голова науково-методичної комісії _____ доц. Володимир ЦИГИКА
(підпис) (прізвище та ініціали)

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	**Розподіл годин за навчальним планом**
	денна форма навчання
Кількість кредитів ЄКТС – 5	Рік підготовки:
Загальна кількість годин – 150	3-й
Кількість модулів – 2	Семестр
	6-й
Тижневих годин для денної форми навчання: аудиторних – 4,6 години самостійної роботи студента – 4,4 години	Лекції
	36 год
	Практичні (семінарські)
	-
Вид підсумкового контролю: екзамен	Лабораторні
	30 год
Форма підсумкового контролю: усна	Самостійна робота
	84 год

2. МЕТА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета вивчення навчальної дисципліни «Захист інформації в комп'ютерних системах» – ознайомлення із організаційними, технічними алгоритмічними та іншими методами і засобами захисту інформації, із законодавством та стандартами в цій області, із сучасними криптосистемами.

Завдання дисципліни – сформувати погляд на захист інформації і криптографію як на систематичну науково-практичну діяльність, що носить прикладний характер. Сформувати базисні теоретичні поняття, що лежать в основі процесу захисту інформації.

Відповідно до освітньої програми «Комп'ютерні системи та мережі», вивчення дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

- інтегральна (здатність розв'язувати складні спеціалізовані задачі та практичні проблеми під час професійної діяльності у комп'ютерній галузі або навчання, що передбачає застосування теорій та методів комп'ютерної інженерії і характеризується комплексністю те невизначеністю умов);
- загальні (ЗК1 здатність до абстрактного мислення, аналізу і синтезу; ЗК2 здатність вчитися і оволодівати сучасними знаннями; ЗК3 здатність застосовувати знання у практичних ситуаціях; ЗК7 Вміння виявляти, ставити та вирішувати проблеми; ЗК8. Здатність працювати в команді);
- фахові (ФК1 здатність застосовувати законодавчу та правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі комп'ютерної інженерії; ФК2 здатність використовувати сучасні методи і мови програмування для розроблення алгоритмічного та програмного забезпечення; ФК3 Здатність створювати системне та прикладне програмне забезпечення комп'ютерних систем та мереж; ФК4 здатність забезпечувати захист інформації, що обробляється в комп'ютерних і кіберфізичних системах та мережах з метою реалізації встановленої політики інформаційної безпеки; ФК 10 Здатність здійснювати організацію робочих місць, їхнє технічне оснащення, розміщення комп'ютерного устаткування, використання організаційних, технічних, алгоритмічних та інших методів і засобів захисту інформації; ФК 15 Здатність аргументувати вибір методів розв'язування спеціалізованих задач, критично оцінювати отримані результати, обґрунтовувати та захищати прийняті рішення).

3. ПЕРЕДУМОВИ ДЛЯ ВИВЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Передумовами вивчення навчальної дисципліни «Захист інформації в комп'ютерних системах» є опанування студентами курсу «Програмування», «Дискретна математика», «Лінійна алгебра та аналітична геометрія», «Теорія інформації і кодування», «Теорія ймовірності і математична статистика», «Комп'ютерна логіка» освітньої програми «Комп'ютерні системи та мережі».

4. ОЧІКУВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Відповідно до освітньої програми «Комп'ютерні системи та мережі», вивчення навчальної дисципліни повинно забезпечити досягнення здобувачами вищої освіти таких програмних результатів навчання (ПРН)**:**

Програмні результати навчання	Шифр ПРН
Знати і розуміти наукові положення, що лежать в основі функціонування комп'ютерних засобів, систем та мереж.	ПРН1
Мати навички проведення експериментів, збирання даних та моделювання в комп'ютерних системах.	ПРН2
Знати новітні технології в галузі комп'ютерної інженерії.	ПРН3
Вміти розв'язувати задачі аналізу та синтезу засобів, характерних для спеціальності.	ПРН7
Вміти системно мислити та застосовувати творчі здібності до формування нових ідей	ПРН8
Вміти ідентифікувати, класифікувати та описувати роботу комп'ютерних систем та їх компонентів.	ПРН 13
Вміти виконувати експериментальні дослідження за професійною тематикою	ПРН15
Вміти оцінювати отримані результати та аргументовано захищати прийняті рішення	ПРН16
Здатність адаптуватись до нових ситуацій обґрунтовувати, приймати та реалізовувати у межах компетенції рішення.	ПРН19
Усвідомлювати необхідність навчання впродовж усього життя з метою поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.	ПРН20

Очікувані результати навчання, які повинні бути досягнуті здобувачами освіти після опанування навчальної дисципліни «Захист інформації в комп'ютерних системах»:

Очікувані результати навчання з дисципліни	Шифр ПРН
Розуміння наукових положень та основних нормативних положень, що лежать у основі організації засобів захисту комп'ютерних систем та мереж. Особливості інформації як об'єкту захисту, перелік та особливості основних загроз інформації в комп'ютерних системах, підходи до розробки політики безпеки комп'ютерної системи, основні принципи захисту інформації, порядок формування комплексу засобів захисту інформації, принципи управління доступом до захищених ресурсів комп'ютерної системи, криптографічні методи і засоби захисту інформації, способи та засоби захисту інформації від витоку технічними каналами, порядок визначення вимог щодо захисту інформації в комп'ютерній системі, основні положення нормативної бази системи захисту інформації в комп'ютерних системах, порядок організації робіт по захисту інформації в комп'ютерних системах.	ПРН1
Вміння застосовувати математичні методи описання і дослідження криптосистем; оцінювати криптографічну стійкість шифрів; проведення експериментів, збирання даних та моделювання в комп'ютерних системах	ПРН2
Знання сучасних методів криптографічного захисту інформації та застосування новітніх технологій у криптології.	ПРН3
Вміння системно мислити та застосовувати творчі здібності до формування нових ідей щодо нових методів засобів захисту	ПРН8
Здійснювати аналіз засобів захисту комп'ютерних систем та мереж. Здійснювати вибіркові атаки на елементи захисту з метою знаходження вразливостей та вирішення наявних проблем	ПРН 13, ПРН15, ПРН16, ПРН 19
Поглиблення набутих та здобуття нових фахових знань, удосконалення креативного мислення.	ПРН20

5. ЗАСОБИ ДІАГНОСТИКИ ТА КРИТЕРІЇ ОЦІНЮВАННЯ РЕЗУЛЬТАТІВ НАВЧАННЯ

Робоча програма з дисципліни «Захист інформації в комп'ютерних системах», що читається на третьому курсі ІТФ спеціальності «комп'ютерна інженерія» має два модулі.

Перший модуль складається з п'яти змістовних модулів ЗМ1(Т1-Т3) ЗМ2 (Т1-Т3), ЗМ3(Т1, Т2). ЗМ4 (Т1,Т2) і ЗМ5 (Т1-Т3), а другий з двох ЗМ6 (Т1-Т3) та ЗМ7 (Т1 – Т3).

Використовуються методи усного контролю та письмового контролю. Поточний контроль передбачає: опитування студентів під час захисту лабораторних робіт та опитування на лекціях; контрольні роботи, індивідуальні, самостійні та тестові завдання. Підсумковий контроль передбачає екзамен.

Для контролю знань розроблено: перелік теоретичних питань, (наведено в додатку); завдання для самостійної роботи, зі змістом яких студенти ознайомлюються на початку семестру.

Оцінка ECTS, яку студент отримує після вивчення кредитного модуля дисципліни, визначається відповідно до рейтингу студента. Рейтинг студента з кредитного модуля складається з балів, що він отримує протягом семестру за такі види робіт:

1. Модульна контрольна робота (МКР) тривалістю по 2 акад. години.
2. Виконання лабораторних робіт.

Протягом семестру студенти виконують 8 лабораторних робіт.

Бали із індивідуальної та самостійної роботи студентів нараховуються за: підготовку рефератів, модернізацію завдань, за творчий підхід до виконання завдань, виконання завдань із удосконалення дидактичних матеріалів з дисципліни.

Сума вагових балів контрольних заходів протягом семестру: 100 балів.

Необхідною умовою допуску до іспиту є відсутність заборгованостей з лабораторних робіт та зарахування контрольних робіт. У кінці вивчення дисципліни виводиться рейтинговий бал, який визначається як середньоарифметичне балів з модулів.

Розподіл балів, які отримують студенти за модуль приведені в таблицях.

Розподіл балів, які отримують здобувачі вищої освіти (модуль 1)

Поточне тестування та самостійна робота													Письмова контроль на робота	Сума
Змістовий модуль 1			Змістовий модуль 2			Змістовий модуль 3		Змістовий модуль 4		Змістовий модуль 5			40	100
Т1	Т2	Т3	Т1	Т2	Т3	Т2	Т3	Т1	Т2	Т1	Т2	Т3		
1	1	2	2	1	1	6	10	10	1	12	1	12		

Розподіл балів, які отримують здобувачі вищої освіти (модуль 2)

Поточне тестування та самостійна робота						Письмова контрольна робота	Сума
Змістовий модуль 6			Змістовий модуль 7			50	100
Т1	Т2	Т3	Т1	Т2	Т3		
12	10	10	4	10	4		

Оцінювання окремих видів навчальної роботи з дисципліни

Вид діяльності здобувача вищої освіти	Модуль 1		Модуль 2	
	Кількість	Максимальна кількість балів (сумарна)	Кількість	Максимальна кількість балів (сумарна)
Лабораторні заняття (виконання та захист)	2	50	3	40
Самостійна робота	1	10	1	10
Модульна контрольна робота	1	40	1	50
Разом		100		100

Критерії оцінювання модульної контрольної роботи

Модульна контрольна робота може проводитись у двох режимах:

- Письмова, яка містить шість завдань. Перші три завдання включають теоретичний або практичний матеріал, наступні 3 завдання – це тести.
- Тестова, що містить 50 тестів із вибором однієї правильної відповіді.

Критерії оцінювання підсумкового семестрового контролю

До складання екзамену допускаються лише студенти, які мають рейтинговий бал не менше 35. Екзамен з навчальної дисципліни студент може не складати, якщо він склав усі модулі та його влаштовує рейтингова оцінка. Студенти, які мають рейтинговий бал від 35 до 59 іспит складають обов'язково. Студент може підвищити на екзамені оцінку, при цьому рейтингова оцінка не може бути зменшена.

За результатами виконання студентом навчальної програми впродовж семестру рекомендується виставляти заліки та екзамени без додаткового опитування за такою шкалою:

Сумарні бали	Оцінка ECTS	Екзамен (диф. залік)	Залік
90 – 100	**A**	Відмінно	Зараховано
82 – 89	**B**	Добре	
74 – 81	**C**		
64 – 73	**D**	Задовільно	
60 – 63	**E**		
35 – 59	**FX**	Незадовільно з можливістю повторного складання	Незараховано з можливістю повторного складання
1 – 34	**F**	Незадовільно з обов'язковим повторним вивченням дисципліни	Незараховано з обов'язковим повторним вивченням дисципліни

6. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

6.1. Зміст навчальної дисципліни

Модуль 1

Змістовий модуль 1. Основи систем захисту інформації у КС.

Тема 1. Зміст базових понять: предмет та об'єкт захисту, вразливість КС. Поняття конфіденційності, цілісності, доступності. Основні види загроз інформаційній безпеці. Зловмисники, класифікація зловмисників. Основи кібербезпеки. Кіберзагрози та кібератаки.

Тема 2. **Організація систем захисту інформації.** Поняття політики безпеки КС. Міри безпеки: нормативно-правові, організаційні, комунікаційно-технічні, програмні. Основні підсистеми комплексу засобів захисту.

Змістовий модуль 2. Концептуальні моделі організації систем захисту інформації в КС.

Тема 1. Математичні моделі політики безпеки. Дискреційної: Модель системи захисту Adept-50. Модель простору безпеки Хартсона. Модель HRU. Модель Take-Grant. **Мандатного доступу***:* Модель системи захисту Бела і Лападули**.** Матриця прав доступу. Потоки запитів суб'єктів до об'єктів. **Модель моніторингу безпеки.** Лічильники небезпечних подій. Вектор індикації аномалій в діях користувача.

Тема 2. Нормативно-правове регулювання інформаційної безпеки. Стандарти США TCSES, GDPR, ISO 27001, Україна НД 25.004-99. Закони України про захист інформації. Кримінальний кодекс України.

Змістовий модуль 3. Управління доступом та розмежування прав доступу до інформації.

Тема 1. Паролі. Ідентифікація та автентифікація користувача. Способи формування та реєстрації паролів. Модифікації системи паролів. Паролі одноразові, ідентифікатори, секретні функції. Двофакторна та багатофакторна автентифікація.

Тема 2. Біометрична ідентифікація та автентифікація.

Тема 3. Механізми контролю доступу (RBAC, DAC, MAC). Протоколи аутентифікації (OAuth, Kerberos, SAML).

Змістовий модуль 4. Основи криптографічного захисту інформації. Симетричні схеми, ключі та системи шифрування.

Тема 1. Базові поняття. Класичні симетричні криптосистеми. Історія виникнення криптографії. Принципи криптографічного захисту інформації. Основні поняття та визначення. Перестановки. Підстановки. Шифри «скітала», Полібія, Цезаря, Плейфера. Шифрувальні таблиці та роторні машини. Шифр Вернама.

Тема 2. Симетричне шифрування. Блокові шифри. Теорія Шеннона, розвиток криптографічних систем. Шифр Фейстеля. Система Люцифер. Стандарт DES, структура алгоритму, основні режими роботи алгоритму: ECB, CBC, OFB, CFB, області застосування, стійкість. Потрійний DES, DESX, S-DES. Алгоритм IDEA. Стандарт ГОСТ 28147-89. Калина. Стандарт AES, ChaCha20**.**

Модуль 2

Змістовий модуль 5. Потокове шифрування.

Тема 1. Потокові шифри та шифри зі змінною довжиною ключа. Blowfish, RC-4, A-5, шифри на основі регістрів зсуву, SEAL, Salsa20.

Тема 2. Генератори ПВП. Випадкові та псевдовипадкові послідовності, їх застосування у криптографії. Найпростіші ГПВП. Сучасні ГПВП. Оцінка якості ГПВП.

Змістовий модуль 6. Асиметричні схеми, ключі та системи шифрування.

Тема 1. Асиметричні криптографічні системи. Елементи теорії чисел. Системи з відкритим ключем. Алгоритм шифрування RSA. Криптосистема Ель-Гамаля. Алгоритми шифрування на основі еліптичних кривих (ECC).

Тема 2. Хеш-згортка повідомлень. Електронний цифровий підпис. Аутентифікація повідомлень. Алгоритми хеш-функцій: MD-5; SHA-3,4; BLAKE2,3**;** Купина та інші. Цифрові підписи: алгоритми EGSA, DSA, RSA та інші.

Тема 3. Управління ключами. Генерування, накопичення, розподіл. Сертифікати відкритих ключів. Сеансові та майстер-ключі. Схема Діффі-Хеллмана розподілення ключів. Протокол обчислення ключа парного зв'язку ECKEP.

Змістовий модуль 7. Сучасні технології інформаційної безпеки

Тема 1. Основи криптоаналізу: основні принципи**,** первинний аналіз, основні методи криптоаналізу.

Тема 2. Стеганографія. Класифікація стеганографічних методів захисту інформації та методи приховування інформації у контейнери різного середовища.

Тема 3. Основні сучасні технології інформаційної безпеки. Гомоморфне шифрування та його застосування. Блокчейн у кібербезпеці. Квантова криптографія. Безпека вебдодатків.

6.2. Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин					
	Денна форма					
	Усього	у тому числі				
		лекції	практичні	лабораторні	індивідуальна робота	самостійна робота
1	2	3	4	5	6	7
Модуль 1						
Змістовий модуль 1. Основи систем захисту інформації у КС						
Тема 1. Зміст базових понять	5	2				3
Тема 2. Організація систем захисту інформації	3	1				2
Разом за змістовим модулем 1	**8**	**3**				**5**
Змістовий модуль 2. Концептуальні моделі організації систем захисту інформації в КС.						
Тема 1. Математичні моделі дискреційної політики безпеки: Модель системи захисту Adept-50. Модель простору безпеки Хартсона. Модель HRU. Модель Take-Grant	8	2				6
Тема 2. Математичні моделі політики мандатного доступу: Модель системи захисту Бела і Лападули. Модель моніторингу безпеки.	8	2				6
Разом за змістовим модулем 2	**16**	**4**				**12**
Змістовий модуль 3. Управління доступом та розмежування прав доступу до інформації						
Тема 1. Паролі. Ідентифікація та аутентифікація користувача.	10	1		6		3
Тема 2. Біометрична ідентифікація та аутентифікація.	5	1				4
Тема 3. Механізми контролю доступу	3	1				2
Разом за змістовим модулем 3	**18**	**3**		**6**		**9**

Змістовий модуль 4. Основи криптографічного захисту інформації. Симетричні схеми, ключі та системи шифрування						
Тема 1. Базові поняття. Історія виникнення криптографії. Принципи криптографічного захисту інформації. Класичні симетричні криптосистеми	20	4		4		12
Тема 2. Симетричне шифрування	14	4		4		6
Разом за змістовим модулем 4	**34**	**8**		**8**		**18**
Разом за модулем 1	**76**	**18**		**14**		**44**
Модуль 2						
Змістовий модуль 5. Потокове шифрування						
Тема 1. Потокові шифри та шифри зі змінною довжиною ключів.	5	1				4
Тема 2. Генератори ПВП.	8	2		2		4
Разом за змістовим модулем 5	**13**	**3**		**2**		**8**
Змістовий модуль 6. Асиметричні схеми, ключі та системи шифрування.						
Тема 1. Асиметричні криптографічні системи: RSA, Ель-Гамаля та інші. Криптостійкість асиметричних та симетричних схем шифрування.	16	4		4		8
Тема 2. Електронний цифровий підпис. Аутентифікація повідомлень. Хеш-згортка повідомлень.	10	2		2		6
Тема 3. Управління ключами. Схема Діфії – Хелмана розподілення ключів.	11	2		4		5
Разом за змістовим модулем 6	**37**	**8**		**10**		**19**
Змістовий модуль 7. Основи криптоаналізу.						
Тема 1. Основи криптоаналізу.	5	2				3
Тема 2. Стеганографія	8	2				6
Тема 3. Сучасні технології інформаційної безпеки	11	3		4		4
Разом за змістовим модулем 7	**24**	**7**		**4**		**13**
Усього за модуль 2	**74**	**18**		**16**		**40**
Усього годин	**150**	**36**		**30**		**84**

6.3. Теми лабораторних занять

№ з/п	Назва теми	Кількість годин
	Модуль 1	
1	Захист інформації за допомогою пароля.	2
2	Розмежування повноважень користувачів на основі парольної автентифікації	4
3	Найпростіші методи шифрування на основі перестановок, підстановок	4
4	Система блочного шифрування S-DES, дослідження властивостей.	4
	Разом за модуль 1	**14**
	Модуль 2	
5	Генерування псевдовипадкових послідовностей	2
6	Використання шифрувальної системи RSA для цифрового підпису	6
7	Відкритий розподіл криптографічних ключів Діффі-Хеллмана	4
8	Комплексне налаштування політик безпеки операційної системи	4
	Разом за модуль 2	**16**
	Разом	**30**

6.4. Самостійна робота

№ з/п	Назва теми	Кількість годин
1	Організація систем захисту інформації.	4
2	Моделі організації систем захисту інформації в КС.	4
3	Історія та класифікація комп’ютерних вірусів.	4
4	Методи захисту від шкідливих програм.	4
5	Основи роботи антивірусних програм.	4
6	Біометрична ідентифікація та аутентифікація.	4
7	Захист ОС мобільних пристроїв.	4
8	Генератори псевдовипадкових чисел.	4
9	Комп’ютерні злочини.	4
10	Основні причини ненадійності криптографічних програм.	4

11	Створення комплексної системи захисту інформації.	4
12	Криптологічний пакет CrypTool.	4
13	Стеганографія.	4
14	Проблеми захисту КС.	4
15	Системи захисту в ОС Linux, Windows.	4
16	Захист інформації в мережах.	4
17	Апаратні та програмно-апаратні засоби захисту інформації в КС.	4
18	Захист програмного забезпечення.	4
	Разом	**76**

7. ІНСТРУМЕНТИ, ОБЛАДНАННЯ ТА ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ВИКОРИСТАННЯ ЯКИХ ПЕРЕДБАЧАЄ НАВЧАЛЬНА ДИСЦИПЛІНА

Лабораторні роботи виконуються на персональних комп'ютерах із встановленою операційною системою Windows, Linux. Програмне забезпечення: пакет Microsoft Windows або LibreOffice, OpenOffice.org, CrypTool. Середовище програмування C#, Python, OpenSSL або інші.

8. РЕКОМЕНДОВАНІ ЛІТЕРАТУРНІ ДЖЕРЕЛА

Основна література

1. Гапак О.М. Захист інформації в комп'ютерних системах: Підручник для студентів спеціальності 123 «комп'ютерна інженерія»/ Гапак О.М. Балога С.І. – Ужгород: «АУТДОР-ШАРК», 2021. – 184с.
2. Гапак О.М. Методичні вказівки і завдання до лабораторних робіт з курсу «Захист інформації в комп'ютерних системах» для студентів 3-4-го курсу інженерно-технічного факультету спеціальності «комп'ютерна інженерія». – Ужгород: «АУТДОР-ШАРК», 2019. – 52 с.
3. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: BHV, 2009. – 608 с.
4. Гундарь К.Ю., Гундарь А.Ю., Янишевський Д.А. Защита информации в компьютерных системах – К.: «Корнейчук», 2010.-152с.
5. Остапов С.Е., Валь Л.О. Основи криптографії: навчальний посібник. Чернівці: Книги–ХХІ, 2008. – 188с.
6. Пірог О.В. Безпека вебдодатків : навч. посібн. / О.В. Пірог. – Електронні дані. – Житомир : Житомирська політехніка, 2025. – 290 с.

Допоміжна література

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015.— 288 с.

2. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C : 20th Anniversary Edition : Wiley, 2015. 784 p.
3. Вишня В. Б. Основи інформаційної безпеки : навч. посіб. / В.Б. Вишня, О.С. Гавриш, Е.В. Рижков. – Дніпро : ДДУВС, 2020. – 128 с.

Додаток 1

Перелік питань до модульного контролю

Модуль 1

1. Предмет та об’єкт захисту.
2, Важливість і складність інформаційної безпеки.
3, Погрози безпеки.
4. Класифікація погроз безпеки.
5. Схеми атак.
6. Організація каналів витоку інформації..
9. Організація систем захисту.
10. Класи безпеки.
11. Моделі системи захисту: мандатна та дискреційна: Модель Adept-50. Модель простору безпеки Хартсона. Модель HRU. Модель Take-Grant, Модель системи захисту Бела і Лападули.
12. Основні поняття ідентифікації та аутентифікація.
13. Застосування пароля для ідентифікації.
14. Біометрична ідентифікація та аутентифікація.
15. Списки доступу. Мандатні списки.
16. Стандарти та критерії для сертифікації. TCSES, ISO 15408-99, НД 2.5.004-
17. Закони України про захист інформації.
18. Кримінальний кодекс. України про захист інформації.
19. Створення комплексної системи захисту інформації.
20. Комп’ютерні злочини. ЇХ класифікація.
21. Організація систем захисту інформації.
22. Модифікації системи паролів. Паролі одноразові, ідентифікатори, секретні функції.
23. Основні принципи криптографічного захисту інформації.
24. Принципи криптографічного захисту інформації.
25. Історія виникнення криптографії.
26. Класифікація методів шифрування(різні підходи).
27. Підстановочні та перестановочні шифри.
28. Шифри Цезаря, Віжінера, Вернама, табличні, Плейфера, Хілла, Гронсфельда та інші.

29. Багатоалфавітна заміна.
30. Дослідження Шеннона в сфері криптології.
31.Сисметричне шифрування. Основні поняття.
32. Деякі відомості із теорії складності задач.
33. Блокові складені шифри. Принцип перемішування, розсіювання.
34. Шифр Фейстеля.
35. DES – алгоритм. Історія виникнення. Загальна схема алгоритму.
36. Структура алгоритму (16 раундів).
37. Режими роботи DES: електронна кодова книга, зчеплення блоків шифру, зворотного зв'язку за шифром, зворотного зв'язку за виходом.
38. Стійкість алгоритму DES.
39. Потрійний DES.
40. DESX.
41. S-DES.
42. Стандарт шифрування ГОСТ 28147-89. Основні ідеї.
43. Порівняння стійкості DES та ГОСТ 28147-89.
44. Алгоритм Blowfish, основні ідеї.
45. Потокові шифри. Загальні відомості.
46. Алгоритм RC4, RC5.
47. Потокові шифри на основі регістрів зсуву.
48. Генератори ПВП.

Модуль 2

1. Криптологічний пакет CrypTool.
2. Хеш-згортка повідомлень. Алгоритми MD-5, SHA, ГОСТ 34.11-94.
3.Зловмисники. Основні напрямки комп'терних злочинів та їх класифікація.
4. Асиметричні криптографічні системи.
5. Алгоритм Евкліда розв'язання рівняння $ax = 1(\mathrm{mod}\, n)$.
6. Алгоритм шифрування RSA. Криптостійкість алгоритму RSA.
7. Криптосистема Ель-Гамаля.
8. Генерування великих простих чисел.
9. Електронний цифровий підпис. Загальні відомості.
10. Функції хешування та їх властивості.
11. Алгоритм цифрового підпису RSA. Недоліки та переваги цифрового підпису RSA.
12. Алгоритм цифрового підпису DSA. Безпека DSA.
13. Алгоритми цифрового підпису ГОСТ Р 34. 10-94, ГОСТ Р 34. 10-2001.
14. Алгоритми цифрового підпису EGSA. Недоліки та переваги цифрового підпису EGSA.
15. Схема сліпого підпису та його застосування.
16. Схема незаперечного підпису та його застосування.
17. Алгоритми сліпого підпису.
18. Алгоритми незаперечного підпису.
19. Управління ключами. Задача обміну ключами.

20. Алгоритм відкритого розподілу ключів Діффі-Хеллмана.
21. Ієрархія ключів. Сертифікати відкритих ключів.
24. Алгоритм розв'язання рівняння $ax = b(\mathrm{mod}\, n)$ за допомого функції Ейлера.
25. Алгоритм розв'язання рівняння $ax = b(\mathrm{mod}\, n)$ за допомого ланцюгових дробів.
26. Стеганографія.
27. Захист ОС мобільних пристроїв.
28. Проблеми захисту КС.
29.Системи захисту в ОС Linux.
30. Основні причини ненадійності криптографічних систем.
31. Апаратні та програмно-апаратні засоби захисту інформації в КС.
32. Захист інформації в мережах.
33. Електронні платіжні системи.
34. Захист програмного забезпечення.
35. Системи захисту в ОС Windows.
36. Основи криптоаналізу.

.

Типові практичні завдання

1. Розшифрувати криптограму «КЛІХТ ВЦТАК ФГШМК НШ ФЗВ БРЩЕЛКЦР», зашифровану на ключі «ШИФРОВКА» шифром Віжінера.
2. Зашифрувати повідомлення «ВИКОРИСТАННЯ ЦЬОГО КАНАЛУ ЗВЯЗКУ НЕБЕЗПЕЧНЕ» табличним методом на ключі «РАЦІЯ».
3. Розшифрувати криптограму «ИСВИЇПНКУАПЬОТ ІРІУВКИТПАЦ», зашифровану табличним методом на ключі «БІРЖА».
4. Зашифрувати повідомлення «ЗУСТРІЧ ПЕРЕНЕСЕМО НА ЗАВТРА» за допомогою шифру Цезаря з ключовим словом «ЗАХИСТ» із зсувом 6 вправо (алфавіт – 32 символи українського алфавіту).
5. Згенерувати псевдовипадкову послідовність із 8 членів за допомогою методу добутків із вихідними значеннями 7 і 23.
6. Згенерувати та визначити період псевдовипадкової послідовності за допомогою LFSR, використовуючи многочлен $x^3 + x^2 + 1$, вхідний блок 1111.
7. Розшифруйте повідомлення C за допомогою алгоритму RSA для таких значень параметрів $p = 5; q = 11; e = 3; C = 9.$
8. Згенерувати спільний ключ для двох користувачів (алгоритм Діффі-Хеллманна) при параметрах $a = 3, p = 10,$ p – модуль системи, a – первісний корінь, секретні ключі користувачів $x_A = 4, x_B = 5$.
9. Розв'язати рівняння $9x = 7(\mathrm{mod}\, 10)$ за допомогою функції Ейлера.
10. Зашифруйте повідомлення M за допомогою алгоритму RSA для таких значень параметрів $p = 11; q = 13; d = 11; M = 7.$